KEY MANAGEMENT TECHNIQUE FOR ESTABLISHING A SECURE CHANNEL

W. Dale Hopkins

ABSTRACT

A key management technique establishes a secure channel through an indeterminate number of nodes in a network. The technique comprises enrolling a smart card with a unique key per smart card. The unique key is derived from a private key that is assigned and distinctive to systems and a card base of a card issuer. An enrolled smart card contains a stored public entity-identifier and the secret unique key. The technique further comprises transacting at a point of entry to the network. The transaction creates a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and transaction sequence number. The technique also comprises communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network, and recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key.